ROM-based computation: quantum versus classical

B. C. Travaglione,[1,*] M. A. Nielsen,[1] H. M. Wiseman,[2] and A. Ambainis[3]

[1] *Centre for Quantum Computer Technology, University of Queensland, St. Lucia, Queensland, Australia*
[2] *School of Science, Griffith University, Nathan, Queensland, Australia*
[3] *Computer Science Division, University of California, Berkeley, USA*

(Dated: September 4, 2001)

We introduce a model of computation which allows us to compare the space-efficiency of reversible, error-free classical computation with reversible, error-free quantum computation. We show that a ROM-based quantum computer with one writable qubit is universal, whilst two writable bits are required for a universal classical ROM-based computer. We also comment on the time-efficiency advantages of quantum computation within this model.

PACS numbers: 03.67.Lx

I. INTRODUCTION

To date, the main drive of research into quantum computation has been to show that the time requirements for solving certain problems are smaller for a quantum computer than they are for a classical computer. Perhaps the most well known result is Shor's algorithm[1], which enables a quantum computer to factor a large integer exponentially faster than can currently be done classically. Other examples of increased time-efficiency using quantum computation are the Deutsch-Jozsa algorithm[2] and Grover's search algorithm[3], both of which provide polynomial speed-ups. For a general introduction to quantum computation, the reader should consult Nielsen and Chuang[4] or Preskill[5].

Whilst time is often considered the key resource to be minimized during the solving of a problem, another resource of considerable importance is space. Space complexity is the study of the number of (qu)bits required by a computer to solve a problem. As is conventional in space complexity theory, we shall differentiate between *read-only* memory and *writable* memory[6]. The space complexity will be a function of the writable memory only. Previous work on space-bounded quantum computation has looked at quantum Turing machines[7] and quantum finite-state automata[8], both of which are bounded-error models. In this paper we introduce a model which allows us to compare the space complexity of error-free, reversible quantum and classical computation.

The structure of this paper is as follows. In Sec. II we explain in detail our ROM-based computation model. In Sec. III we prove that a ROM-based quantum computer with one writable qubit is universal. In section Sec. IV we prove that two writable bits are required for a universal classical ROM-based computer. Finally, in Sec. V we comment on time-efficiency within the model.

*Electronic address: btrav@physics.uq.edu.au

II. ROM-BASED COMPUTATION

In this paper we are considering mappings between strings of boolean variables (bits) of the following form,

$$u_1 u_2 \dots u_j \underbrace{00\dots0}_{n \text{ (qu)bits}} \xrightarrow{F} u_1 u_2 \dots u_j f_1 f_2 \dots f_n, \quad (1)$$

where each $u_i \in \{0,1\}$ and each $f_i \in \{0,1\}$. It is evident from Eq. (1) that the first j bits have the same initial and final values, however in our model, we shall require that the values of the first j bits are also not altered during any of the steps of the computation, so we can consider them to be *read-only memory* or ROM bits. Each of the last n bits are mapped to zero or one, depending on the values of the ROM bits. Therefore we can think of each of these n bits as *writable* bits, whose final value is a boolean function of the ROM-bits,

$$f_i(u_1, u_2, \dots, u_j) \; : \; \mathbb{B}_2^j \to \mathbb{B}_2 \quad i \in \{1, 2, \dots, n\}. \quad (2)$$

In the classical case, a given function f_i is generated by a sequence of arbitrary classical *reversible* gates acting on the n writable bits. Additionally, any of these gates can be applied conditionally upon the value of *one* of the j ROM bits. We are using only reversible gates to preserve the number of writable bits. Any irreversible gate which increases the number of writable bits (e.g. FANOUT) has an associated space complexity cost, whilst irreversible gates which reduce the number of writeable bits (e.g. AND) can be simulated using reversible gates at no space complexity cost.

In the quantum case, arbitrary quantum gates can be applied to the n qubits, and once again any of these gates can be applied conditionally upon the value of *one* of the j ROM bits. However, it should be remembered that each of the f_i are boolean expressions, thus whilst the qubits can exist in superpositional states during the computation, at the conclusion they must be in a computational basis state. This means that the entire computation (including measurement) is deterministic and reversible, as measuring the n qubits at the end of the computation will have no effect on their state[15].

It is perhaps natural to question why we are allowing a given gate to be conditional on only *one* of the ROM bits. Generally, in both quantum and classical computation, arbitrary numbers of controls are allowed[16], as these can always be broken down into gates containing a fixed number of controls (two in the case of quantum computation[9], and three in the case of classical computation[10]). However, breaking down such conditional gates requires the conditional bits to be writable, and therefore has an associated space complexity cost. It should also be pointed out that there is nothing unique about allowing only one control ROM bit per gate. The results presented in the paper would be unaffected by allowing any *fixed* number of simultaneous conditional ROM bits.

Throughout this paper we shall be using circuit diagrams to represent our ROM-based computations. As is standard in quantum computational circuit diagrams, the writable (qu)bits will be represented as horizontal lines, whose states change as various gates are applied from left to right. The ROM bits will be depicted above the circuit diagram, with a line from a ROM bit to a gate implying that this gate is applied only if the ROM bit has value one. Fig. 1 contains an example of a ROM computation circuit diagram. This diagram depicts the computation

$$u_1u_2u_3|0\rangle|0\rangle \xrightarrow{F} u_1u_2u_3|f_1\rangle|f_2\rangle, \tag{3}$$

where

$$\begin{aligned} |f_1(u_1,u_3)\rangle &= |u_1\oplus u_3\rangle \quad \text{and} \\ |f_2(u_1,u_2)\rangle &= |u_1\oplus u_1u_2\rangle. \end{aligned} \tag{4}$$

Please note that we shall be using kets to denote the writable elements of a ROM-based computer, irrespective of whether these elements are bits or qubits.

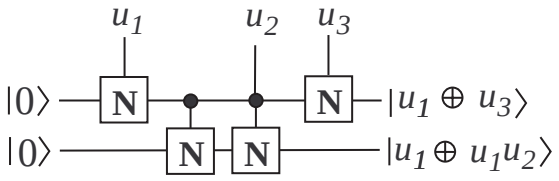

FIG. 1: An example of a ROM-based circuit diagram, the boxes indicate NOT gates and the circles indicate controls. The variables at the top of the diagram are the ROM bits.

We shall define as *universal* a ROM-based computer which is capable of transforming the n writable (qu)bits to any one of the $2\hat{}(n2^j)$ possible boolean outputs. In Sec. III we prove that *one* writable qubit is sufficient for a universal ROM-based quantum computer, whilst in Sec. IV we show that *two* writable bits are required for a universal ROM-based classical computer. In either the classical or quantum case it is easy to see that if the ROM model is universal with m writable (qu)bits then it is universal for any $m' \geq m$, so the main interest is in determining the minimal m for which universality holds.

The proofs contained in the following sections depend upon the fact that XOR and conjunction produce a distinguished normal form. In order to define this distinguished normal form, let us first review some propositional logic theory. It is well known that AND and negation are sufficient to express any boolean proposition[11]. Using the three simple equivalences,

$$\begin{aligned} 1a &\equiv a \\ \bar{a} &\equiv a\oplus 1 \\ a(b\oplus c) &\equiv ab\oplus ac, \end{aligned} \tag{5}$$

it follows that AND and XOR are also sufficient, as every negated sentence, $\bar{a}$, can be replaced by $a\oplus 1$. This implies that all $2\hat{}(2^j)$ propositions composed of j boolean variables can be express as an XOR disjunction of conjunctions, involving no negations. Hence, XOR and AND produce a *normal form*. XOR and AND also produce a *distinguished normal form*, as every expression involving only XOR disjunctions of conjunctions, with no negations, is unique up to transposition of conjunctions. To see that each expression is unique, we note that there are exactly $\binom{j}{k}$ distinct conjunctions involving exactly k of j variables. Thus, the total number of conjunctions is $\sum_{k=0}^{j}\binom{j}{k}=2^j$. The presence or absence of each of these terms gives the $2\hat{}(2^j)$ different boolean propositions.

To prove that a ROM-based computer is universal, we need to show that each writable (qu)bit can be mapped from 0 to any of the $2\hat{}(2^j)$ different boolean propositions. As every boolean expression can be written as an XOR disjunction of conjunctions, it is sufficient to show that we can transform $|f\rangle$ to $|f\oplus u_1u_2\ldots u_m\rangle$ where f is an arbitrary boolean function and $m\in\{1,2,\ldots,j\}$.

III. ONE WRITABLE QUBIT IS UNIVERSAL

We will now use the Pauli operators,

$$Z=\begin{pmatrix}1&0\\0&-1\end{pmatrix} \text{ and } X=\begin{pmatrix}0&1\\1&0\end{pmatrix}, \tag{6}$$

as well as the operators $X^{-\frac{1}{2}}, X^{\frac{1}{2}}, Z^{-\frac{1}{2}}$ and $Z^{\frac{1}{2}}$ to show that a ROM-based quantum computer with one writable qubit is universal. We denote by W_{u_i} an operator W which is applied conditionally on the ROM bit u_i. The sequence of one-qubit gates,

$$X_{u_i}^{-\frac{1}{2}}Z_{u_j}X_{u_i}^{\frac{1}{2}}Z_{u_j} = iX_{u_iu_j} \tag{7}$$

performs a bit flip *if and only if* ROM bits $u_i=u_j=1$. Evidently, if both u_i and u_j are zero, no gate is performed, whilst if only one of u_i or u_j is one, then a gate is performed, followed immediately by its inverse, leaving

the writable qubit unaltered. However, if both u_i and u_j are one, the sequence of four gates combine to give the Pauli X matrix, which has the effect of flipping the qubit in the computational basis. A circuit diagram for this computation is depicted in Fig. 2(a), whilst Fig. 2(b) shows how a qubit initial in the state $|0\rangle$ is transformed into the state $|1\rangle$ iff $u_i = u_j = 1$. Thus, the sequence in

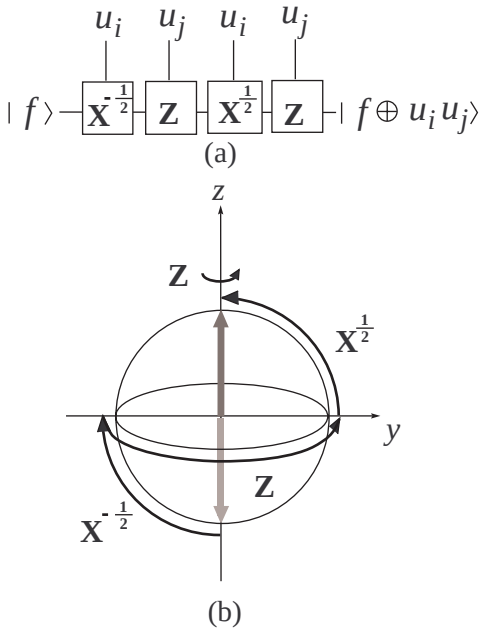

FIG. 2: (a) Circuit diagram of the ROM sequence used to transform $|f\rangle$ to $|f \oplus u_i u_j\rangle$. (b) Bloch sphere representation showing the state $|0\rangle$ transforming to the state $|1\rangle$, when $u_i = u_j = 1$. For all other values of u_i and u_j, $|f\rangle$ remains unchanged.

Eq. (7) takes a writable qubit from $|f\rangle$ to $|f \oplus u_i u_j\rangle$.

Now each of the Z_{u_j} terms in Eq. (7) can be replaced by

$$Z_{u_k}^{-\frac{1}{2}} X_{u_j} Z_{u_k}^{\frac{1}{2}} X_{u_j} \;=\; i Z_{u_k u_j}, \tag{8}$$

which gives the sequence

$$X_{u_i}^{-\frac{1}{2}} Z_{u_j u_k} X_{u_i}^{\frac{1}{2}} Z_{u_j u_k} \;=\; X_{u_i u_j u_k}, \tag{9}$$

ignoring an overall phase factor. This new sequence of gates takes $|f\rangle$ to $|f \oplus u_i u_j u_k\rangle$. By replacing the X_{u_j} terms in Eq. (8) by sequences of the form given in Eq. (7) it is easy to see, by recursion, that we can generate a sequence of gates which transforms $|f\rangle$ to $|f \oplus u_1 u_2 \ldots u_m\rangle$. This completes our proof that a ROM-based quantum computer with one writable qubit is universal.

IV. TWO WRITABLE BITS ARE UNIVERSAL

Consider a ROM-based classical computer with one writable bit. The only allowable operations are a NOT gate, N, and a conditional NOT gate, N_{u_i}. Any combination of these two gates will not be able to transform $|f\rangle$ to $|f \oplus u_i u_j\rangle$, therefore a one bit ROM-based classical computer is not universal. This results also follows from a theorem by Toffoli[12].

Now consider a ROM-based classical computer with two writable bits. The four gates depicted in Fig. 3 perform the transforms

$$|\alpha\rangle|\beta\rangle \xrightarrow{N_{u_i}^{(1)}} |\alpha \oplus u_i\rangle|\beta\rangle \tag{10a}$$

$$|\alpha\rangle|\beta\rangle \xrightarrow{N_{u_i}^{(2)}} |\alpha\rangle|\beta \oplus u_i\rangle \tag{10b}$$

$$|\alpha\rangle|\beta\rangle \xrightarrow{C_{u_i}^{(1)}} |\alpha \oplus u_i\beta\rangle|\beta\rangle \tag{10c}$$

$$|\alpha\rangle|\beta\rangle \xrightarrow{C_{u_i}^{(2)}} |\alpha\rangle|\beta \oplus u_i\alpha\rangle. \tag{10d}$$

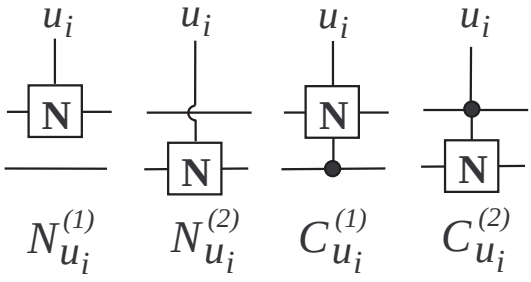

FIG. 3: Circuit diagram representation of the four transforms given in Eq. (10).

We now wish to prove, using the four transforms from Eq. (10) that it is possible to transform the writable bits from the state $|\alpha\rangle|\beta\rangle$ to $|\alpha\rangle|\beta \oplus u_1 u_2 \ldots u_m\rangle$. Let us denote by S_0 the gate $N_{u_1}^{(1)}$, which takes $|\alpha\rangle|\beta\rangle$ to $|\alpha \oplus u_1\rangle|\beta\rangle$. It is not hard to show that the sequence

$$S_1 \;:\; C_{u_2}^{(2)} S_0 C_{u_2}^{(2)} S_0 \tag{11}$$

performs the transform

$$|\alpha\rangle|\beta\rangle \xrightarrow{S_1} |\alpha\rangle|\beta \oplus u_1 u_2\rangle. \tag{12}$$

Now, suppose we have a sequence of gates, S_{m-1}, which performs the transform

$$|\alpha\rangle|\beta\rangle \xrightarrow{S_{m-1}} |\alpha\rangle|\beta \oplus u_1 u_2 \ldots u_{m-1}\rangle. \tag{13}$$

Then there exists a sequence of gates,

$$S_m \;:\; C_{u_m}^{(1)} S_{m-1} C_{u_m}^{(1)} S_{m-1} \tag{14}$$

which perform the transform

$$|\alpha\rangle|\beta\rangle \xrightarrow{S_m} |\alpha \oplus u_1 u_2 \ldots u_m\rangle|\beta\rangle. \tag{15}$$

This completes the proof.

V. TIME EFFICIENCY

A simple counting argument shows that there exists boolean expressions which will require an exponential number of ROM calls on either a quantum or classical ROM computer with a fixed number of writeable (qu)bits. However, it is an open question as to whether there exist specific boolean expressions which can be generated on a one qubit quantum computer using a polynomial number of ROM calls, which require an exponential number of ROM calls on a two bit classical computer. Consider the transform

$$|f\rangle \to |f \oplus u_1 u_2 \dots u_j\rangle. \tag{16}$$

Eq. (7) indicates that the transform $|f\rangle \to |f \oplus u_1 u_2\rangle$ can be accomplished using four ROM calls. Now, by making the following replacements,

$$X_{u_1}^{-\frac{1}{2}} \text{ with } X_{u_1}^{-\frac{1}{4}} Z_{u_2} X_{u_1}^{\frac{1}{4}} Z_{u_2} \tag{17a}$$

$$X_{u_1}^{\frac{1}{2}} \text{ with } X_{u_1}^{\frac{1}{4}} Z_{u_2} X_{u_1}^{-\frac{1}{4}} Z_{u_2} \tag{17b}$$

$$Z_{u_2} \text{ with } Z_{u_3}^{-\frac{1}{2}} X_{u_4} Z_{u_3}^{\frac{1}{2}} X_{u_4}, \tag{17c}$$

we can transform $|f\rangle \to |f \oplus u_1 u_2 u_3 u_4\rangle$ using 16 ROM calls. A direct extension of this method, replacing each $X^{\pm 1/2^n}$ by

$$X^{\mp 1/2^{n+1}} Z X^{\pm 1/2^{n+1}} Z, \tag{18}$$

and each $Z^{\pm 1/2^n}$ by

$$Z^{\mp 1/2^{n+1}} X Z^{\pm 1/2^{n+1}} X, \tag{19}$$

allows us to take the AND of up to 2^k ROM bits using exactly 4^k ROM calls. Thus, to take the AND of $O(j)$ ROM bits requires only $O(j^2)$ quantum gates. (Note that if the number of ROM bits is not a power of two we need simply include some dummy ROM bits set equal to 1.)

Using a result by Barrington[13], on the power of width-5 branching programs, we can show that the transform

$$|f\rangle|g\rangle|h\rangle \to |f \oplus u_1 u_2 \dots u_j\rangle|g\rangle|h\rangle \tag{20}$$

can be performed effeciently on a classical ROM computer. However, the power of a width-4 branching program appears to be much less, thus we conjecture[17] that the transform

$$|f\rangle|g\rangle \to |f \oplus u_1 u_2 \dots u_j\rangle|g\rangle. \tag{21}$$

requires $O(2^j)$ ROM calls on a two bit classical computer.

If our model allowed the ability to clear the writable bits (an irreversible step), then we can transform $|f\rangle|0\rangle$ to $|f \oplus u_1 u_2 \dots u_j\rangle|0\rangle$ on a classical two bit computer using only j ROM calls. The circuit for this computation is shown in Fig. 4, where the circles denotes re-initialization of the bit.

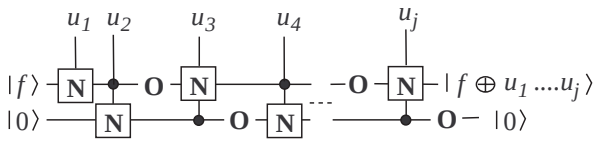

FIG. 4: A circuit diagram showing the efficient transformation of $|f\rangle$ to $|f \oplus u_1 u_2 \dots u_j\rangle$ on an irreversible classical ROM computer. The circles indicate re-initialization.

It is perhaps worth noting that time efficiency of multiple controlled-NOT gates have been investigated by Barenco et al.[14], where they find the number of required basic gates scales quadratically with the circuit size. However they use the fact that all the (qu)bits in the network are writeable.

VI. DISCUSSION

In conclusion, we have introduced a model, which allows the comparison of space-efficiency between error-free, reversible quantum and classical computation. We have shown that quantum computation is more space efficient within this model, requiring only one qubit for universality, as opposed to two bits. We have also conjectured that the minimal quantum ROM computer can calculate certain boolean functions exponentially faster than the minimal classical ROM computer.

It would be interesting to compare the classical and quantum models, allowing for bounded-error computation, that is, the writeable bits are mapped to the correct boolean functions of the ROM bits with some probability $1 - \epsilon$. Preliminary investigations indicate that the quantum model would still be more powerful than the classical model.

[1] P. W. Shor, Proc. 35th Annual Symposium on Foundations of Computer Science p. 124 (1994).

[2] D. Deutsch and R. Jozsa, Proceedings of the Royal Society of London A **439**, 553 (1992).

[3] L. K. Grover, Physical Review Letters **79**, 325 (1997).

[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[5] J. Preskill, *Quantum Information and Computation*, California Institute of Technology, Pasadena, CA, USA (1998).
[6] C. H. Papadimitriou, *Computational Complexity* (Addison - Wesley, Reading, Massachusetts, 1994).
[7] J. Watrous, Journal of Computer and Systems Sciences **59**, 281 (1999).
[8] A. Ambainis and R. Freivalds, Proceedings of FOCS'98 (1998).
[9] D. P. DiVincenzo, Physical Review A **51**, 1015 (1995).
[10] E. Fredkin and T. Toffoli, International Journal of Theoretical Physics **21**, 219 (1982).
[11] D. Hilbert and W. Ackermann, *Principles of Mathematical Logic* (Chelsea Publishing Co., USA, 1950).
[12] T. Toffoli, in *Automata, Languages and Programming*, edited by J. W. de Bakker and J. van Leeuwen (1980), p. 632.
[13] D. A. Barrington, Journal of Computer and System Sciences **38**, 150 (1989).
[14] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Physical Review A **52**, 3457 (1995).
[15] Intermediate measurements can be made in neither the quantum or classical models, as the storing of the measurement result would be effectively expanding the workspace.
[16] If arbitrary numbers of controls are allowed it is trivial to show that a one (qu)bit ROM computer is universal.
[17] This conjecture is based on numerical tests for small values of j. A proof will be difficult to find, as we need to show that no required circuits of ploynomial length exist.